UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/589,766	08/17/2006	Frederic Beun	MM6020PCT	9662

79681 7590 09/20/2011

David A. Einhorn, Esq.
Baker & Hostetler LLP
45 Rockefeller Plaza
New York, NY 10111

EXAMINER	
AVERY, JEREMIAH L	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
09/20/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

deinhorn@bakerlaw.com
Patents-BakerHostetler@bakerlaw.com
IPGNYG@bakerlaw.com

Office Action Summary	Application No.	Applicant(s)	
	10/589,766	BEUN ET AL.	
	Examiner	Art Unit	
	JEREMIAH AVERY	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 June 2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-59* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-59* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *13 October 2010* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

I. Claims 57-59 have been added.

II. Claims 1-59 have been examined.

III. Responses to Applicant's remarks have been given.

Response to Arguments

1. The objection and 35 U.S.C. 112, second paragraph rejection of claim 3 are hereby withdrawn due to the Applicant's amendments to said claim. Further, the subsequent 35 U.S.C. 112, second paragraph rejection of claims 4-14 is also hereby withdrawn.

2. The objections to claims 22-27 and 45-56 are hereby withdrawn due to the Applicant's amendments.

3. The Applicant states that "the process identification values of Risan are not used for matching (pairing) matching N data reception equipments with M external security modules as is set forth in claim 1..."; however, in response to Applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Further, Risan does disclose this via, inter alia, page 1, paragraph 9, "a list of process identification values".

4. Also, the Applicant argues that "Risan does not teach verifying: whether or not the identifier of an external security module is present in the list memorized in the reception equipment and, whether or not the identifier of said reception equipment is

present in the list memorized in said external security module, consistent with the check phase of claim 1". However, Risan was not cited to disclose these claimed features, but rather Hirota was utilized for disclosing said claimed features, as cited below.

5. Further the Applicant claims that the priority date of February 20th, 2004; however the PALM system indicates that the priority of the Application is February 17th, 2005; thus Risan's filing date of July 8th, 2004 permits Risan to be used as prior art.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1-5, 14-20, 38 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent No. 6,606,707 to Hirota et al., hereinafter Hirota and further in view of United States Patent Application Publication No. US 2006/0021057 to Risan et al., hereinafter Risan.

6. Regarding claim 1, Hirota teaches a method for matching a number N of data reception equipment with a number M of external security modules, each reception equipment being provided with a unique identifier, and each external security module having a unique identifier (column 3, lines 3-8 and column 5, lines 9-20),
method characterised in that it comprises a configuration phase comprising the following steps:
memorizing a list of identifiers of reception equipment in each data external security module (column 5, lines 9-17, "an identification information storage unit which stores a piece of identification information identifying an electronic device"),
and carrying out a check phase when an external security module is connected to data reception equipment, comprising the following steps:
whether or not the identifier for said reception equipment is present in the list of identifiers memorized in said external security module, and if so, authorizing access to data using said external security module and said reception equipment, and if not, preventing access to the distributed data by means of said external security module with said reception equipment (column 3, lines 3-15, "mutual authentication", column 5, lines 9-32, "prevents the occurrence of unauthorized tapping and using of the personal data" and lines 55-67 and column 6, lines 1-10).

7. Hirota teaches the claimed invention, as cited above. However, it does not teach the claim language pertaining to "memorizing a list of identifiers of external security module in each reception equipment, verifying whether or not the identifier for said

external security module is present in the list of identifiers memorized in said reception equipment". Risan teaches said claim language, as cited below.

8. Regarding claim 1, Risan teaches memorizing a list of identifiers of external security modules in each reception equipment, verifying whether or not the identifier for said external security module is present in the list of identifiers memorized in said reception equipment (page 1, paragraph 9, "a list of process identification values" and page 6, paragraph 71).

9. The motivation to combine to provide "a system for preventing unauthorized reproduction of media disposed on a media storage device" (*Risan* – page 1, paragraph 9).

10. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Risan with the teachings of Hirota so as to ensure that access to specific data only occurs when the proper equipment is utilized.

11. Regarding claim 2, Hirota teaches that the configuration is used only when the user connects an external security module to a reception equipment (column 5, lines 33-54).

12. Regarding claim 3, Hirota teaches that the method also comprises a step in which an operator transmits a signal to the reception equipment to manage the check phase comprising *one of the following* set values: activating the check phase at *or* after a programmed delay, deactivating the check phase at *or* after a programmed delay,

specifying an absolute date in which the check phase is activated *or* deactivated, cancelling said programmed date (column 10, lines 50-65).

13. Regarding claim 4, Hirota teaches that an operator also transmits a signal to the reception equipment containing a message to delete the list of identifiers memorised in the reception equipment (Figure 14C, column 7, lines 16-18).

14. Regarding claims 5, 40-42, Hirota teaches that an operator also transmits to the external security module a signal containing a message to delete the list of identifiers memorised in this external security module (column 4, lines 60-64, "destroying the semiconductor memory card", column 20, lines 58-67 and column 21, lines 1-14).

15. Regarding claim 14, Hirota teaches the operator transmits a signal message for the check phase to a group of reception equipment in a private flow, said private flow being processed by a dedicated software executable in each reception equipment as a function of the identifier of said reception equipment (column 3, lines 3-15, "mutual authentication", column 5, lines 9-32, "prevents the occurrence of unauthorized tapping and using of the personal data" and lines 55-67 and column 6, lines 1-10).

16. Hirota significantly teaches the claimed invention, as cited above. However, Hirota does not substantially teach the claim language of claim 15. Risan teaches said claim language, as cited below.

17. Regarding claim 15, Risan teaches that the list of identifiers of external security module is transmitted in a private flow to a group of reception equipment and processed by a dedicated software executable in each reception equipment as a function of the

identifier of said reception equipment (page 1, paragraph 9, "a list of process identification values" and page 6, paragraph 71).

18. The motivation to combine to provide "a system for preventing unauthorized reproduction of media disposed on a media storage device" (*Risan* – page 1, paragraph 9).

19. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Risan with the teachings of Hirota so as to ensure that access to specific data only occurs when the proper equipment is utilized.

20. Regarding claim 16, Hirota teaches that the list of identifiers of reception equipment is transmitted to a group of external security modules in a private flow that is processed by a dedicated software in each of said external security modules *or* in the reception equipment to which each of said external security modules is connected, as a function of the identifier of said external security module (column 3, lines 36-52 and column 5, lines 9-17, "an identification information storage unit which stores a piece of identification information identifying an electronic device").

21. Regarding claim 17, Hirota teaches that digital data are distributed in plain text *or* in scrambled form (column 9, lines 10-16 and 45-57).

22. Hirota teaches the claimed invention, as cited above. However, Hirota does not teach the claim language found within claim 19. Risan teaches said claim language, as cited below.

23. Regarding claim 19, Risan teaches that the list of identifiers of M security modules memorised in a reception equipment is encrypted (page 10, paragraph 97, "the messages being passed back and forth between client computer system 210 and web server 250 can also be encrypted, thereby protecting the media files and the data being exchanged from unauthorized use or access").

24. The motivation to combine to provide "a system for preventing unauthorized reproduction of media disposed on a media storage device" (*Risan* – page 1, paragraph 9).

25. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Risan with the teachings of Hirota so as to ensure that access to specific data only occurs when the proper equipment is utilized.

26. Regarding claim 20, Hirota teaches that the list of identifiers of N reception equipment memorised in an external security module is encrypted (column 4, lines 19-32).

27. Regarding 38, Hirota discloses an access control system including a plurality of reception equipment each having a unique identifier and that can cooperate with a plurality of external security modules each having a unique identifier, each external security module containing information about access rights of a subscriber to digital data distributed by an operator, said system also including a commercial management platform communicating with said reception equipment and said external security modules, characterised in that is also includes: a first module arranged in said

commercial platform and designed to generate matching queries (column 3, lines 3-15, "mutual authentication", column 5, lines 9-32, "an identification information storage unit which stores a piece of identification information identifying an electronic device" and "prevents the occurrence of unauthorized tapping and using of the personal data" and lines 55-67 and column 6, lines 1-10).

28. Hirota significantly discloses the claimed invention, as cited above. However, Hirota does not substantially disclose the claim language of "a second module arranged in said reception equipment and in said external security modules and designed to process said queries to prepare a matching configuration". Risan discloses said claim language, as cited below.

29. Regarding claim 38, Risan discloses a second module arranged in said reception equipment and in said external security modules and designed to process said queries to prepare a matching configuration (page 1, paragraph 9).

30. The motivation to combine to provide an access control method which prevents fraudulent equipment from being utilized due to tampering with the identifiers of acceptable equipment.

31. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Risan with the teachings of Hirota so as to ensure that access to specific data only occurs when the proper equipment is utilized.

32. Regarding claim 39, Hirota discloses a computer program stored in memory executable on N reception equipment that can cooperate with M security modules each

having a unique identifier and in which information about access rights of a subscriber to digital data distributed by an operator are stored, characterised in that it comprises instructions for memorising a list of identifiers of *part or all* of N reception equipment in each external security module (column 5, lines 9-17, "an identification information storage unit which stores a piece of identification information identifying an electronic device"),

instructions to prevent access to said data if the identifier of the security module connected to the reception equipment is not present in the list of identifiers previously memorised in this reception equipment *or* if the identifier of said reception equipment is not present in the list of identifiers previously memorised in said external security module (column 3, lines 3-15, "mutual authentication", column 5, lines 9-32, "prevents the occurrence of unauthorized tapping and using of the personal data" and lines 55-67 and column 6, lines 1-10).

33. Hirota significantly discloses the claimed invention, as cited above. However, Hirota does not disclose the claimed invention with regards to the claim language of "instructions to memorise a list of identifiers of part or all of the M external security modules in each reception equipment, instructions to control the identifier of a security module connected to a reception equipment and the identifier of said reception equipment". Risan discloses said claim language, as cited below.

34. Regarding claim 39, Risan discloses instructions to memorise a list of identifiers of part or all of the M external security modules in each reception equipment, instructions to control the identifier of a security module connected to a reception

equipment and the identifier of said reception equipment (page 1, paragraph 9, "a list of process identification values" and page 6, paragraph 71).

35. The motivation to combine to provide "a system for preventing unauthorized reproduction of media disposed on a media storage device" (*Risan* – page 1, paragraph 9).

36. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Risan with the teachings of Hirota so as to ensure that access to specific data only occurs when the proper equipment is utilized.

37. Claims 6-13, 18, 21, 25-27 and 43-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirota and Risan as applied to claim 1 above, and further in view of United States Patent No. 6,405,369 to Tsuria, hereinafter Tsuria.

38. Hirota and Risan teach the claimed invention, as cited above. However, Hirota and Risan do not teach the claim language within claims 6-13, 21, 43-45, 49 and 53 pertaining to "an EMM message". Tsuria teaches said claim language, as cited below.

39. [As it is known, an EMM (Entitlement Management Message) provides conditional access information pertaining to the authority that a viewer/receiver has in receiving the particular transmissions and services of a content provider. Tsuria's disclosure of the "deactivation dates" being "communicated to the first smart card and to the second smart card via the pay television network" is interpreted by the Examiner to pertain to a notification that states the duration in which the smart cards can be used to help provide access to the television broadcasts.]

40. The motivation to combine would be to provide the means to ensure "preventing the smart card from performing the access control functions" (*Tsuria* – column 5, lines 15-18).

41. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Tsuria with the teachings of Hirota and Risan to provide "a pay television access control method to be employed in a pay television system in which pay television programs are transmitted to a plurality of subscribers, each being entitled to receive selected programs" (*Tsuria* – column 3, lines 20-25).

42. The motivation and obviousness to combine pertains to claims 6-13, 21-27 and 43-59.

43. Regarding claim 6, Tsuria teaches that an operator transmits the list of M identifiers of the external security modules to a reception equipment through an EMM message specific to said reception equipment (column 6, lines 9-19, 32-47 and 55-59, column 7, lines 11-23 and 44-67).

44. Regarding claim 7, Tsuria teaches that the operator transmits an list of identifiers of N reception equipment to an external security module through an EMM message specific to said external security module (column 6, lines 9-19, 32-47 and 55-59, column 7, lines 11-23 and 44-67).

45. Regarding claims 8, 43, 44, Tsuria teaches that an operator transmits the list of M identifiers of external security modules to a group of reception equipment through an

EMM message specific to said group of reception equipment (column 6, lines 9-19, 32-47 and 55-59, column 7, lines 11-23 and 44-67).

46. Regarding claim 9, Tsuria teaches that the operator transmits the list of identifiers of N reception equipment to a group of external security modules through an EMM message specific to said group of external security modules (column 6, lines 9-19, 32-47 and 55-59, column 7, lines 11-23 and 44-67).

47. Regarding claim 10, Tsuria teaches that the operator supplies said signal message to a reception equipment through an EMM message specific to said reception equipment (column 6, lines 9-19, 32-47 and 55-59, column 7, lines 11-23 and 44-67).

48. Regarding claim 11, Tsuria teaches that the operator supplies said signal message to a group of reception equipment through an EMM message specific to said group of reception equipment (column 6, lines 9-19, 32-47 and 55-59, column 7, lines 11-23 and 44-67).

49. Regarding claim 12, Tsuria teaches that the operator supplies said signal message to an external security module through an EMM message specific to said external security module (column 6, lines 9-19, 32-47 and 55-59, column 7, lines 11-23 and 44-67).

50. Regarding claim 13, Tsuria teaches that the operator supplies said signal message to a group of external security modules through an EMM message specific to said group of external security modules (column 6, lines 9-19, 32-47 and 55-59, column 7, lines 11-23 and 44-67).

51. Regarding claims 21, 49 and 53, Tsuria teaches that the method also includes a mechanism designed to prevent use of an EMM transmitted to the same external security module or to the same reception equipment (column 7, lines 11-23 and column 9, lines 34-40).

52. Regarding claims 22, 46, 50 and 54, Tsuria teaches that said EMM is in the following format:

EMM-U section()

Table_id = 0x88 8 bits

section_syntax_indicator = 0 1 bit

DVB_reserved 1 bit

ISO reserved 2 bits

EMM-U_section_length 12 bits

unique_address_field 40 bits

for (i=0; i<N; i++)

EMM_data_byte 8 bits (column 6, lines 9-19, 32-47 and 55-59, column 7, lines 11-23 and 44-67).

53. Regarding claims 23, 47, 51 and 55, Tsuria teaches that said EMM message concerns all external security modules (6,8) or all reception equipment (2) and is in the following format:

EMM-G section()

Table_id = 0x8A or 0x8B 8 bits

section_syntax_indicator = 0 1 bit

DVB_reserved 1 bit

ISO reserved 2 bits

EMM-G_section_length 12 bits

for (i=0; i<N; i++)

EMM_data_byte 8 bits (column 6, lines 9-19, 32-47 and 55-59, column 7, lines 11-23 and 44-67).

54. Regarding claims 24, 48, 52 and 56, Tsuria teaches that said EMM message is specific to a sub-group of external security modules (6,8) or a sub-group of reception equipment (2) and is in the following format:

EMM-S section()

Table_id = 0x8E 8 bits

section_syntax_indicator = 0 1 bit

DVB_reserved 1 bit

ISO reserved 2 bits

EMM-S_section_length 12 bits

Shared_address_field 24 bits

reserved 6 bits

Data_format 1 bit

ADF_scrambling_flag 1 bit

for (i=0; i<N; i++)

EMM_data_byte 8 bits (column 6, lines 9-19, 32-47 and 55-59, column 7, lines 11-23 and 44-67).

55. Regarding claims 25 and 57, Tsuria teaches that the equipment includes a decoder and in that the external security module is an access control card containing information about access rights of a subscriber to said digital data, matching being done between said decoder and said card (column 1, lines 50-65, column 3, lines 20-29 and column 5, lines 24-29).

56. Regarding claims 26 and 58, Tsuria teaches that the equipment includes a decoder and in that the external security module is a removable security interface provided with a non-volatile memory and designed to cooperate firstly with said decoder, and secondly with a plurality of conditional access control cards, to manage access to said digital data, matching being done between said decoder and said removable security interface (column 1, lines 50-65, column 3, lines 20-29 and column 5, lines 24-61).

57. Regarding claims 27 and 59, Tsuria teaches that the equipment includes a decoder provided with a removable security interface with a non-volatile memory and designed to cooperate firstly with said decoder, and secondly with a plurality of conditional access control cards and in that matching is done between said removable security interface and said access control cards (column 2, lines 43-67, column 3, lines 1-19 and 50-67 and column 4, lines 1-38).

58. Hirota and Risan teach the claimed invention, as cited above. However, Hirota and Risan do not teach the claim language of claim 18. Tsuria teaches said claim language, as cited below.

59. Regarding claim 18, Tsuria teaches that digital data are audiovisual programs (column 1, lines 50-60, "pay television transmissions").

60. The motivation to combine would be to allow for the system to provide access to the desired type of data.

61. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Tsuria with the teachings of Hirota and Risan to provide "a pay television access control method to be employed in a pay television system in which pay television programs are transmitted to a plurality of subscribers, each being entitled to receive selected programs" (*Tsuria* – column 3, lines 20-25).

62. Claims 28-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent No. 6,405,369 to Tsuria, hereinafter Tsuria and further in view of United States Patent Application Publication No. US 2006/0021057 to Risan et al., hereinafter Risan.

63. Regarding claim 28, Tsuria teaches a reception equipment that can be matched with a plurality of external security modules to manage access to digital data distributed by an operator (column 1, lines 50-60, "pay television transmissions").

64. Tsuria teaches the claimed invention, as cited above. However, Tsuria does not teach the claim language pertaining to "a non-volatile memory designed to memorise a list of external security modules, means of verifying if the identifier of an external security module connected to said equipment is present in the list memorised in said non-volatile memory". Risan teaches said claim language, as cited below.

65. Regarding claim 28, Risan teaches in that it includes: a non-volatile memory designed to memorise a list of external security modules, means of verifying if the identifier of an external security module connected to said equipment is present in the list memorised in said non-volatile memory (Figure 1, element 103, "Non-Volatile Memory", page 3, paragraph 44 and page 6, paragraph 71).

66. The motivation to combine to provide "a system for preventing unauthorized reproduction of media disposed on a media storage device" (*Risan* – page 1, paragraph 9).

67. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Risan with the teachings of Hirota so as to ensure that access to specific data only occurs when the proper equipment is utilized.

68. Regarding claim 29,Tsuria teaches that the equipment includes a decoder and in that the external security module is an access control card containing information about access rights of a subscriber to said digital data, matching being done between said decoder and said card (column 1, lines 50-65, column 3, lines 20-29 and column 5, lines 24-29).

69. Regarding claim 30, Tsuria teaches that the equipment includes a decoder and in that the external security module is a removable security interface provided with a non-volatile memory and designed to cooperate firstly with said decoder, and secondly with a plurality of conditional access control cards, to manage access to said digital data,

matching being done between said decoder and said removable security interface (column 1, lines 50-65, column 3, lines 20-29 and column 5, lines 24-61).

70. Regarding claim 31, Tsuria teaches that the equipment includes a decoder provided with a removable security interface with a non-volatile memory and designed to cooperate firstly with said decoder, and secondly with a plurality of conditional access control cards and in that matching is done between said removable security interface and said access control cards (column 2, lines 43-67, column 3, lines 1-19 and 50-67 and column 4, lines 1-38).

71. Regarding claim 32, Tsuria teaches a Decoder that can cooperate with a plurality of external security modules to manage access to audiovisual programs distributed by an operator (column 1, lines 50-60, "pay television transmissions").

72. Tsuria teaches the claimed invention, as cited above. However, Tsuria does not teach the claim language with regards to "each external security module having a single identifier and comprising at least one data processing algorithm, decoder characterized in that it includes: a non-volatile memory designed to memorise a list of external security modules, means of verifying if the identifier of an external security module connected to said decoder is present in the list memorised in said non-volatile memory". Risan teaches said claim language, as cited below.

73. Regarding claim 32, Risan teaches each external security module having a single identifier and comprising at least one data processing algorithm, decoder characterized in that it includes: a non-volatile memory designed to memorise a list of external security modules, means of verifying if the identifier of an external security

module connected to said decoder is present in the list memorised in said non-volatile memory (Figure 1, element 103, "Non-Volatile Memory", page 1, paragraph 9, "a list of process identification values", page 3, paragraph 44 and page 6, paragraph 71).

74. The motivation to combine to provide "a system for preventing unauthorized reproduction of media disposed on a media storage device" (*Risan* – page 1, paragraph 9).

75. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Risan with the teachings of Hirota so as to ensure that access to specific data only occurs when the proper equipment is utilized.

76. Regarding claim 33, Tsuria teaches that said external security modules are access control cards in which information about access rights of a subscriber to digital data distributed by an operator is memorized (column 1, lines 50-65, column 3, lines 20-29, column 5, lines 24-61 and column 6, lines 9-15).

77. Regarding 34, Tsuria teaches that said external security modules are removable security interfaces including a non-volatile memory and designed to cooperate firstly with the decoder, and secondly with a plurality of conditional access control cards to manage access to digital data distributed by an operator (column 1, lines 50-65, column 3, lines 20-29 and column 5, lines 24-61).

Claim Rejections - 35 USC § 102

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

78. Claims 35-37 are rejected under 35 U.S.C. 102(b) as being anticipated by United States Patent No. 6,606,707 to Hirota et al., hereinafter Hirota.

79. Regarding claim 35, Hirota discloses a removable security interface designed to cooperate firstly with a reception equipment, and secondly with a plurality of conditional access control cards, to manage access to digital data distributed by an operator, each card having a unique identifier and containing information about access rights of a subscriber to said digital data, interface characterised in that it includes: a non-volatile memory designed to memorise a list of subscriber cards, means of verifying if the identifier of a card associated with said interface is present in the list memorised in said non-volatile memory (column 3, lines 3-15, "mutual authentication", column 5, lines 9-32, "an identification information storage unit which stores a piece of identification information identifying an electronic device" and "prevents the occurrence of unauthorized tapping and using of the personal data" and lines 55-67 and column 6, lines 1-10).

80. Regarding claim 36, Hirota discloses that it consists of a PCMCIA card containing a digital data descrambling software (column 7, lines 61-67 and column 8, lines 38-57).

81. Regarding claim 37, Hirota discloses that it consists of a software (column 7, lines 61-67 and column 8, lines 9-19, 31-34 and 38-57).

Conclusion

82. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

83. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

84. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

United States Patent No. 6,366,585 to Dapper et al., which is cited to show distributed control in a communication system.

United States Patent No. 6,330,241 to Fort which is cited to show multi-point to point communication system with remote unit burst identification.

United States Patent No. 6,334,219 to Hill et al., which is cited to show channel selection for a hybrid fiber coax network.

United States Patent No. 6,292,651 to Dapper et al., which is cited to show a communication system with multicarrier transport distribution network between a head end terminal and remote units.

United States Patent No. 5,625,693 to Rohatgi et al., which is cited to show an apparatus and method for authenticating transmitting applications in an interactive tv system.

United States Patent No. 5,485,221 to Banker et al., which is cited to show a subscription television system and terminal for enabling simultaneous display of multiple services.

United States Patent No. 6,061,057 to Knowlton et al., which is cited to show a network commercial system using visual link objects.

United States Patent No. 7,181,010 to Russ et al., which is cited to show an apparatus for entitling remote client devices.

United States Patent No. 6,438,550 to Doyle et al., which is cited to show a method and apparatus for client authentication and application configuration via smart cards.

United States Patent No. 6,405369 to Tsuria, which is cited to show smart card chaining in pay television systems.

85. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEREMIAH AVERY whose telephone number is (571)272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

86. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

87. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jeremiah Avery/
Examiner, Art Unit 2431

/NATHAN FLYNN/
Supervisory Patent Examiner, Art Unit 2431